Desktop Management Guide

Business Desktops dx5150 Series

Document Part Number: 375370-002

February 2005

This guide provides definitions and instructions for using security and Intelligent Manageability features that are preinstalled on select models.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

WARNING: Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

Desktop Management Guide
Business Desktops dx5150 Series

First Edition (December 2004)
Second Edition (February 2005)

Document Part Number: 375370-002

Contents

Desktop Management Guide

HP Intelligent Manageability provides standards-based solutions for managing and controlling desktops, workstations, and notebook PCs in a networked environment. HP pioneered desktop manageability in 1995 with the introduction of the industry's first fully manageable desktop personal computers. HP is a patent holder of manageability technology. Since then, HP has led an industry-wide effort to develop the standards and infrastructure required to effectively deploy, configure, and manage desktops, workstations, and notebook PCs. HP works closely with leading management software solution providers in the industry to ensure compatibility between Intelligent Manageability and these products. Intelligent Manageability is an important aspect of our broad commitment to providing you with PC Lifecycle Solutions that assist you during the four phases of the desktop PC lifecycle—planning, deployment, management, and transitions.

The key capabilities and features of desktop management are:

- Initial configuration and deployment
- Remote system installation
- Software updating and management
- ROM flash
- Asset tracking and security
- Fault notification and recovery

Initial Configuration and Deployment

The computer comes with a preinstalled system software image. After a brief software “unbundling” process, the computer is ready to use.

You may prefer to replace the preinstalled software image with a customized set of system and application software. There are several methods for deploying a customized software image. They include:

- Installing additional software applications after unbundling the preinstalled software image.
- Using software deployment tools, such as Altiris Deployment Solution™, to replace the preinstalled software with a customized software image.
- Using a disk cloning process to copy the contents from one hard drive to another.

The best deployment method depends on your information technology environment and processes. The PC Deployment section of the HP Lifecycle Solutions Web site (http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html) provides information to help you select the best deployment method.

The *Restore Plus!* CD, ROM-based setup, and ACPI hardware provide further assistance with recovery of system software, configuration management and troubleshooting, and power management.

Remote System Installation

Remote System Installation allows you to set up the system using the software and configuration information located on a network server by initiating the Preboot Execution Environment (PXE). The Remote System Installation feature is usually used as a system setup and configuration tool, and can be used for the following tasks:

- Formatting a hard drive
- Deploying a software image on one or more new PCs
- Remotely updating the system BIOS in flash ROM ("Remote ROM Flash" on page 7)
- Configuring the system BIOS settings

To initiate Remote System Installation, press **F12** when the F12 = Network Service Boot message appears in the lower-right corner of the HP logo screen. Follow the instructions on the screen to continue the process. The default boot order is a BIOS configuration setting that can be changed to always attempt to PXE boot.

HP and Altiris have partnered to provide tools designed to make the task of corporate PC deployment and management easier and less time-consuming, ultimately lowering the total cost of ownership and making HP PCs the most manageable client PCs in the enterprise environment.

Software Updating and Management

HP provides several tools for managing and updating software on desktops and workstations—HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification; and Subscriber's Choice.

HP Client Manager Software

HP Client Manager Software (HP CMS) assists HP customers in managing the hardware aspects of their client computers with features that include:

- Detailed views of hardware inventory for asset management
- PC health check monitoring and diagnostics
- Proactive notification of changes in the hardware environment
- Web-accessible reporting of business critical details such as machines with thermal warnings, memory alerts, and more
- Remote updating of system software such as device drivers and ROM BIOS
- Remote changing of boot order
- Configuring the system BIOS settings

For more information on the HP Client Manager, visit http://www.hp.com/go/im .

Altiris Client Management Solutions

HP and Altiris have partnered to provide comprehensive, tightly integrated systems management solutions to reduce the cost of owning HP client PCs. HP Client Manager Software is the foundation for additional Altiris Client Management Solutions that address:

- Inventory and Asset Management
  - ❏ SW license compliance
  - ❏ PC tracking and reporting
  - ❏ Lease contract, fixing asset tracking
- Deployment and Migration
  - ❏ Microsoft Windows XP Professional or Home Edition migration
  - ❏ System deployment
  - ❏ Personality migrations

- Help Desk and Problem Resolution
    - ❏ Managing help desk tickets
    - ❏ Remote troubleshooting
    - ❏ Remote problem resolution
- Software and Operations Management
    - ❏ Ongoing desktop management
    - ❏ HP system SW deployment
    - ❏ Application self-healing

For more information and details on how to download a fully-functional 30-day evaluation version of the Altiris solutions, visit http://h18000.www1.hp.com/im/prodinfo.html#deploy.

On selected desktop and notebook models, an Altiris management agent is included as part of the factory loaded image. This agent enables communication with the Altiris Development Solution which can be used to complete new hardware deployment or personality migration to a new operating system using easy-to-follow wizards. Altiris solutions provide easy-to-use software distribution capabilities. When used in conjunction with System Software Manager, or HP Client Manager Software, administrators can also update ROM BIOS and device driver software from a central console.

For more information, visit http://www.hp.com/go/EasyDeploy.

System Software Manager

System Software Manager (SSM) is a utility that lets you update system-level software on multiple systems simultaneously. When executed on a PC client system, SSM detects both hardware and software versions, then updates the appropriate software from a central repository, also known as a file store. Driver versions that are supported by SSM are denoted with a special icon on the software and driver download Web site and on the Support Software CD. To download the utility or to obtain more information on SSM, visit http://www.hp.com/go/ssm.

Proactive Change Notification

The Proactive Change Notification program uses the Subscriber's Choice Web site in order to proactively and automatically:

- Send you Proactive Change Notification (PCN) e-mails informing you of hardware and software changes to most commercial computers and servers, up to 60 days in advance.
- Send you e-mail containing Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins, and Driver alerts for most commercial computers and servers.

You create your own profile to ensure that you only receive the information relevant to a specific IT environment. To learn more about the Proactive Change Notification program and create a custom profile, visit http://www.hp.com/go/pcn.

Subscriber’s Choice

Subscriber’s Choice is a client-based service from HP. Based on your profile, HP will supply you with personalized product tips, feature articles, and/or driver and support alerts/notifications. Subscriber’s Choice Driver and Support Alerts/Notifications will deliver e-mails notifying you that the information you subscribed to in your profile is available for review and retrieval. To learn more about Subscriber’s Choice and create a custom profile, visit http://www.hp.com/go/pcn.

ROM Flash

The computer comes with a programmable flash ROM (read only memory). By establishing a Supervisor password in the Computer Setup (F10) Utility, you can protect the ROM from being unintentionally updated or overwritten. This is important to ensure the operating integrity of the computer.

Should you need or want to upgrade the ROM, you may:

- Order an upgraded ROMPaq diskette from HP.
- Download the latest ROMPaq images from HP driver and support page, http://www.hp.com/support/files.

CAUTION: For maximum ROM protection, be sure to establish a Supervisor password. The Supervisor password prevents unauthorized ROM upgrades. System Software Manager allows the system administrator to set the Supervisor password on one or more PCs simultaneously. For more information, visit http://www.hp.com/go/ssm.

Remote ROM Flash

Remote ROM Flash allows the system administrator to safely upgrade the ROM on remote HP computers directly from the centralized network management console. Enabling the system administrator to perform this task remotely, on multiple computers and personal computers, results in a consistent deployment of and greater control over HP PC ROM images over the network. It also results in greater productivity and lower total cost of ownership.

✎ The computer must be powered on, or turned on through Remote Wakeup, to take advantage of Remote ROM Flash.

For more information on Remote ROM Flash, refer to the HP Client Manager Software or System Software Manager at http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

The HPQFlash utility is used to locally update or restore the system ROM on individual PCs through a Windows operating system.

For more information on HPQFlash, visit http://www.hp.com/support/files and enter the name of the computer when prompted.

FailSafe Boot Block ROM

The FailSafe Boot Block ROM allows for system recovery in the unlikely event of a ROM flash failure, for example, if a power failure were to occur during a ROM upgrade. The Boot Block is a flash-protected section of the ROM that checks for a valid system ROM flash when power to the system is turned on.

- If the system ROM is valid, the system starts normally.
- If the system ROM fails the validation check, the FailSafe Boot Block ROM provides enough support to start the system from a ROMPaq diskette, which will program the system ROM with a valid image.

✎ Some models also support recovery from a ROMPaq CD.

When the boot block detects an invalid system ROM, the System Power LED blinks RED 8 times, one every second, followed by a 2-second pause. Also 8 simultaneous beeps will be heard. A Boot Block recovery mode message is displayed on the screen (some models).

✎ The beeps continue through five cycles of 8 simultaneous beeps and stop; however, the LED continues blinking until the issue is resolved.

To recover the system after it enters Boot Block recovery mode, complete the following steps:

1. If there is a diskette in the diskette drive or a CD in the CD drive, remove the diskette and CD and turn off the power.
2. Insert a ROMPaq diskette into the diskette drive or, if permitted on this computer, a ROMPaq CD into the CD drive.

3. Turn on the computer.

   If no ROMPaq diskette or ROMPaq CD is found, you will be prompted to insert one and restart the computer.

   If a supervisor password has been established, the Caps Lock light will turn on and you will be prompted to enter the password.

4. Enter the supervisor password.

   If the system successfully starts from the diskette or CD and successfully reprograms the ROM, then the three keyboard lights will turn on. A rising tone series of beeps also signals successful completion.

5. Remove the diskette or CD and turn the power off.
6. Turn the power on again to restart the computer.

The following table lists the various keyboard light combinations used by the Boot Block ROM (when a PS/2 keyboard is attached to the computer), and explains the meaning and action associated with each combination.

Keyboard Light Combinations Used by Boot Block ROM

FailSafe Boot Block Mode	Keyboard LED Color	Keyboard LED Activity	State/Message
Num Lock	Green	On	ROMPaq diskette or ROMPaq CD not present, is bad, or drive not ready.
Caps Lock	Green	On	Enter password.
Num, Caps, Scroll Lock	Green	Blink On in sequence, one at a time—N, C, SL	Keyboard locked in network mode.
Num, Caps, Scroll Lock	Green	On	Boot Block ROM Flash successful. Turn power off, then on to reboot.

✎ Diagnostic lights do not flash on USB keyboards.

Replicating the Setup

To replicate or copy one setup configuration to other computers of the same model, HP has provided a Windows-based software utility, System Software Manager, that can be downloaded from http://www.hp.com/go/ssm, plus a DOS-based software, CMOS Save/Load utility, that can be downloaded from http://www.hp.com/support/files. After logging on to the HP Support Web site, enter the name of your computer when prompted.

Creating a Bootable Device

Supported USB Flash Media Device

Supported devices, such as an HP Drive Key, have a preinstalled image to simplify the process of making them bootable. If the USB flash media device being used does not have this image, use the procedure later in this section (see "Unsupported USB Flash Media Device" on page 13).

⚠ **CAUTION:** Not all computers can be booted from a USB flash media device. If the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive, the computer can be booted from a USB flash media device. Otherwise, a bootable diskette must be used.

To create a bootable USB flash media device, you must have:

- an HP Business Desktop dx5150 Series - Microtower, Small Form Factor, or Slim Tower.

  Depending on the individual BIOS, future systems may also support booting to a USB flash media device.
- a 256MB HP Drive Key II storage module.
- A bootable DOS diskette with the FDISK and SYS programs. If SYS is not available, FORMAT may be used, but all existing files on the USB flash media device will be lost.

1. Turn off the computer.
2. Insert the USB flash media device into one of the computer's USB ports and remove all other USB storage devices except USB diskette drives.

3. Insert a bootable DOS diskette with FDISK.COM and either SYS.COM or FORMAT.COM into a diskette drive and turn on the computer to boot to the DOS diskette.

4. Run FDISK from the A:\ prompt by typing **FDISK** and pressing **Enter.** If prompted, click **Yes** (**Y**) to enable large disk support.

5. Enter Choice [**5**] to display the drives in the system. The USB flash media device will be the drive that closely matches the size of one of the drives listed. It will usually be the last drive in the list. Note the letter of the drive.

   USB flash media device drive: __________

△ **CAUTION:** If a drive does not match the USB flash media device, do not proceed. Data loss can occur. Check all USB ports for additional storage devices. If any are found, remove them, reboot the computer, and proceed from step 4. If none are found, either the system does not support the USB flash media device or the USB flash media device is defective. DO NOT proceed in attempting to make the USB flash media device bootable.

6. Exit FDISK by pressing the **Esc** key to return to the A:\ prompt.

7. If your bootable DOS diskette contains SYS.COM, go to step 8. Otherwise, go to step 9.

8. At the A:\ prompt, enter **SYS x:** where x represents the drive letter noted above.

△ **CAUTION:** Be sure that you have entered the correct drive letter for the USB flash media device.

   After the system files have been transferred, SYS will return to the A:\ prompt. Go to step 13.

9. Copy any files you want to keep from your USB flash media device to a temporary directory on another drive (for example, the system's internal hard drive).

10. At the A:\ prompt, enter **FORMAT /S X:** where X represents the drive letter noted before.

△ **CAUTION:** Be sure that you have entered the correct drive letter for the USB flash media device.

FORMAT will display one or more warnings and ask you each time whether you want to proceed. Enter **Y** each time. FORMAT will format the USB flash media device, add the system files, and ask for a Volume Label.

11. Press **Enter** for no label or enter one if desired.
12. Copy any files you saved in step 9 back to your USB flash media device.
13. Remove the diskette and reboot the computer. The computer will boot to the USB flash media device as drive C.

✎ The default boot order varies from computer to computer, and it can be changed in the Computer Setup (F10) Utility.

If you have used a DOS version from Windows 9x, you may see a brief Windows logo screen. If you do not want this screen, add a zero-length file named LOGO.SYS to the root directory of the USB flash media device.

Unsupported USB Flash Media Device

△ **CAUTION:** Not all computers can be booted from a USB flash media device. If the default boot order in the Computer Setup (F10) Utility lists the USB device before the hard drive, the computer can be booted from a USB flash media device. Otherwise, a bootable diskette must be used.

To create a bootable USB flash media device, you must have:

- an HP Business Desktop dx5150 Series - Microtower, Small Form Factor or Slim Tower.

  Depending on the individual BIOS, future systems may also support booting to a USB flash media device.

- A bootable DOS diskette with the FDISK and SYS programs. If SYS is not available, FORMAT may be used, but all existing files on the USB flash media device will be lost.

1. If there are any PCI cards in the system that have SCSI, ATA RAID or SATA drives attached, turn off the computer and unplug the power cord.

△ **CAUTION:** The power cord MUST be unplugged.

2. Open the computer and remove the PCI cards.
3. Insert the USB flash media device into one of the computer's USB ports and remove all other USB storage devices except USB diskette drives. Close the computer cover.
4. Plug in the power cord and turn on the computer.
5. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

6. Go to **Integrated Peripherals > South OnChip IDE Device** to disable the PATA controller, and go to **Integrated Peripherals > South OnChip PCI Device** to disable the SATA controller. Exit setup, confirming the changes.
7. Insert a bootable DOS diskette with FDISK.COM and either SYS.COM or FORMAT.COM into a diskette drive and turn on the computer to boot to the DOS diskette.
8. Run FDISK and delete any existing partitions on the USB flash media device. Create a new partition and mark it active. Exit FDISK by pressing the **Esc** key.
9. If the system did not automatically restart when exiting FDISK, press **Ctrl+Alt+Del** to reboot to the DOS diskette.
10. At the A:\ prompt, type **FORMAT C: /S** and press **Enter.** Format will format the USB flash media device, add the system files, and ask for a Volume Label.
11. Press **Enter** for no label or enter one if desired.
12. Turn off the computer and unplug the power cord. Open the computer and re-install any PCI cards that were previously removed. Close the computer cover.
13. Plug in the power cord, remove the diskette, and turn on the computer.
14. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.
15. Go to **Integrated Peripherals > South OnChip IDE Device** and **Integrated Peripherals > South OnChip PCI Device** and re-enable the PATA and SATA controllers that were disabled in step 6.
16. Save the changes and exit. The computer will boot to the USB flash media device as drive C.

✎ The default boot order varies from computer to computer, and it can be changed in the Computer Setup (F10) Utility. Refer to the *Computer Setup Guide* on the *Documentation CD* for instructions.

If you have used a DOS version from Windows 9x, you may see a brief Windows logo screen. If you do not want this screen, add a zero-length file named LOGO.SYS to the root directory of the USB flash media device.

Dual-State Power Button

With Advanced Configuration and Power Interface (ACPI) enabled, the power button can function either as an on/off switch or as a standby button. The standby feature does not completely turn off power, but instead causes the computer to enter a low-power standby state. This allows you to power down quickly without closing applications and to return quickly to the same operational state without any data loss.

To change the power button's configuration, complete the following steps:

1. Left click on the **Start Button,** then select **Control Panel > Power Options.**
2. In the **Power Options Properties,** select the **Advanced** tab.
3. In the **Power Button** section, select **Standby**.

After configuring the power button to function as a standby button, press the power button to put the system in a very low power state (standby). Press the button again to quickly bring the system out of standby to full power status. To completely turn off all power to the system, press and hold the power button for four seconds.

△ **CAUTION:** Do not use the power button to turn off the computer unless the system is not responding; turning off the power without operating system interaction could cause damage to or loss of data on the hard drive.

World Wide Web Site

HP engineers rigorously test and debug software developed by HP and third-party suppliers, and develop operating system specific support software, to ensure performance, compatibility, and reliability for HP computers.

When making the transition to new or revised operating systems, it is important to implement the support software designed for that operating system. If you plan to run a version of Microsoft Windows that is different from the version included with the computer, you must install corresponding device drivers and utilities to ensure that all features are supported and functioning properly.

HP has made the task of locating, accessing, evaluating, and installing the latest support software easier. You can download the software from http://www.hp.com/support.

The Web site contains the latest device drivers, utilities, and flashable ROM images needed to run the latest Microsoft Windows operating system on the HP computer.

Building Blocks and Partners

HP management solutions integrate with other systems management applications, and are based on industry standards, such as:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LAN Technology
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) support

Asset Tracking and Security

Asset tracking features incorporated into the computer provide key asset tracking data that can be managed using HP Systems Insight Manager, HP Client Manager Software or other system management applications. Seamless, automatic integration between asset tracking features and these products enables you to choose the management tool that is best suited to the environment and to leverage the investment in existing tools.

HP also offers several solutions for controlling access to valuable components and information. ProtectTools Embedded Security, if installed, prevents unauthorized access to data and checks system integrity and authenticates third-party users attempting system access. (Refer to *HP ProtectTools Embedded Security Guide,* on the *Documentation CD* for more information.) A Security feature such as ProtectTools helps to prevent unauthorized access to the internal components of the personal computer. By disabling parallel, serial, or USB ports, or by disabling removable media boot capability, you can protect valuable data assets. Memory Change events can be automatically forwarded to system management applications to deliver proactive notification of tampering with a computer's internal components.

✎ ProtectTools is available on some systems.

Use the following utilities to manage security settings on the HP computer:

- Locally, using the Computer Setup Utilities. See the *Computer Setup (F10) Utility Guide* on the *Documentation CD* included with the computer for additional information and instructions on using the Computer Setup Utilities.
- Remotely, using HP Client Manager Software or System Software Manager. This software enables the secure, consistent deployment and control of security settings from a simple command-line utility.

The following table and sections refer to managing security features of the computer locally through the Computer Setup (F10) Utilities.

Security Features Overview

Option	Description
Supervisor Password	Allows you to set and enable Supervisor (administrator) password. ✎ If the Supervisor password is set, it is required to change Computer Setup options, flash the ROM, and make changes to certain plug and play settings under Windows. See the *Troubleshooting Guide* on the *Documentation CD* for more information.
User Password	Allows you to set and enable a User password. ✎ If the User password is set, it is required to access the computer when power is turned on. See the *Troubleshooting Guide* on the *Documentation CD* for more information.
Device Security	Enables/disables serial ports, parallel port, front USB ports, system audio, and network controllers (some models).

✎ For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide* on the *Documentation CD*.

Support for security features may vary depending on the specific computer configuration.

Security Features Overview *(Continued)*

Option	Description
Network Service Boot	Enables/disables the computer's ability to boot from an operating system installed on a network server. (Feature available on NIC models only; the network controller must reside on the PCI bus or be embedded on the system board.)
System IDs	Allows you to set: • Asset tag (18-byte identifier) and ownership Tag (80-byte identifier displayed during POST). • Chassis serial number or Universal Unique Identifier (UUID) number. The UUID can only be updated if the current chassis serial number is invalid. (These ID numbers are normally set in the factory and are used to uniquely identify the system.) Keyboard locale setting (for example, English or German) for System ID entry.

✎ For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide* on the *Documentation CD*.

Support for security features may vary depending on the specific computer configuration.

Security Features Overview *(Continued)*

Option	Description
Master Boot Record Security	Allows you to enable or disable Master Boot Record (MBR) Security. When enabled, the BIOS rejects all requests to write to the MBR on the current bootable disk. Each time the computer is powered on or rebooted, the BIOS compares the MBR of the current bootable disk to the previously-saved MBR. If changes are detected, you are given the option of saving the MBR on the current bootable disk, restoring the previously-saved MBR, or disabling MBR Security. You must know the setup password, if one is set. ✎ Disable MBR Security before intentionally changing the formatting or partitioning of the current bootable disk. Several disk utilities (such as FDISK and FORMAT) attempt to update the MBR. If MBR Security is enabled and disk accesses are being serviced by the BIOS, write requests to the MBR are rejected, causing the utilities to report errors. If MBR Security is enabled and disk accesses are being serviced by the operating system, any MBR change will be detected by the BIOS during the next reboot, and an MBR Security warning message will be displayed.

✎ For more information about Computer Setup, see the *Computer Setup (F10) Utility Guide* on the *Documentation CD.*

Support for security features may vary depending on the specific computer configuration.

Password Security

The User password prevents unauthorized use of the computer by requiring entry of a password to access applications or data each time the computer is turned on or restarted. The Supervisor password specifically prevents unauthorized access to Computer Setup, and can also be used as an override to the User password. That is, when prompted for the User password, entering the Supervisor password instead will allow access to the computer.

A network-wide setup password can be established to enable the system administrator to log in to all network systems to perform maintenance without having to know the User password.

✎ System Software Manager and HP Client Manager Software allow remote management of Setup Passwords and other BIOS settings in a networked environment. For more information, visit http://www.hp.com/go/EasyDeploy.

Establishing a Supervisor Password Using Computer Setup

If the system is equipped with an embedded security device, refer to *HP ProtectTools Embedded Security Guide,* on the *Documentation CD*. Establishing a Supervisor password through Computer Setup prevents reconfiguration of the computer (use of the Computer Setup F10 utility) until the password is entered.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart.**
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Set Supervisor Password** and enter the password on the screen.
4. Before exiting, click **File > Save Changes and Exit.**

Establishing a User Password Using Computer Setup

Establishing a User password through Computer Setup prevents access to the computer when power is turned on, unless the password is entered. When a User password is set, Computer Setup presents Password Options under the Security menu. Password options include Password Prompt on Warm Boot. When Password Prompt on Warm Boot is enabled, the password must also be entered each time the computer is rebooted.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart.**
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Set User Password** and enter the password on the screen.
4. Before exiting, click **File > Save Changes and Exit.**

Entering a User Password

To enter a User password, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the **Enter Password** box appears on the monitor, type the current password, then press **Enter.**

✎ Type carefully; for security reasons, the characters you type do not appear on the screen.

If you enter the password incorrectly, the message “Invalid Password, Press any key to continue!” appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

Entering a Supervisor Password

If the system is equipped with an embedded security device, refer to *HP ProtectTools Embedded Security Guide,* on the *Documentation CD*.

If a Supervisor password has been established on the computer, you will be prompted to enter it each time you run Computer Setup.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart.**
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. When the **Enter Password** box appears on the monitor, type the Supervisor password, then press **Enter**.

✎ Type carefully; for security reasons, the characters you type do not appear on the screen.

If you enter the password incorrectly, the message “Invalid Password, Press any key to continue!” appears. Try again. After three unsuccessful tries, you must turn off the computer, then turn it on again before you can continue.

Changing a User or Supervisor Password

If the system is equipped with an embedded security device, refer to *HP ProtectTools Embedded Security Guide,* on the *Documentation CD*.

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart the Computer.**
2. When the **Enter Password** box appears, type the current User password, if a password is required.
3. Press **Enter.**
4. Press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

5. When the **Enter Password** box appears to access Computer Setup, type the current Supervisor password, if required.
6. Press **Enter.**
7. Select either **Set Supervisor Password** or **Set User Password.**
8. When the **Enter Password** box appears on the screen, type the new password and press **Enter.**
9. Before exiting, click **File > Save Changes and Exit.**

✎ To delete a password instead of changing it, when the **Enter Password** box appears on the screen, press **Enter** instead of entering the new password. This deletes the current password.

Clearing Passwords

If you forget the password, you cannot access the computer. Refer to the *Troubleshooting Guide* on the *Documentation CD* for instructions on clearing passwords.

If the system is equipped with an embedded security device, refer to *HP ProtectTools Embedded Security Guide,* on the *Documentation CD*.

Master Boot Record Security

The Master Boot Record (MBR) contains information needed to successfully boot from a disk and to access the data stored on the disk. Master Boot Record Security detects and reports unintentional or malicious changes to the MBR, such as those caused by some computer viruses or by the incorrect use of certain disk utilities. It also allows you to recover the “last known good” MBR, should changes to the MBR be detected when the system is restarted.

To enable MBR Security, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart.**
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Advanced BIOS Features > MBR Security** and press **Enter.**
4. In the MBR Security Pop-up box, press the up or down arrows to select **Enabled** or **Disabled.**
5. To accept the changes, press **Enter.** To abort the changes, press the **Esc** key.

When MBR Security is enabled, the BIOS prevents any changes being made to the MBR of the current bootable disk while in MS-DOS or Windows Safe Mode.

✎ Most operating systems control access to the MBR of the current bootable disk; the BIOS cannot prevent changes that may occur while the operating system is running.

Each time the computer is turned on or restarted, the BIOS compares the MBR of the current bootable disk to the previously saved MBR. If changes are detected and if the current bootable disk is the same disk from which the MBR was previously saved, the following message is displayed:

1999—Master Boot Record has changed.

1. Press any key to enter Setup to configure MBR Security.
2. Upon entering Computer Setup, you must disable the MBR Security feature.

You must know the Supervisor password, if one exists.

If changes are detected and if the current bootable disk is **not** the same disk from which the MBR was previously saved, the following message is displayed:

2000—Master Boot Record Hard Drive has changed.

1. Press any key to enter Setup to configure MBR Security.
2. Upon entering Computer Setup, you must disable the MBR Security feature.

You must know the Supervisor password, if one exists.

In the unlikely event that the previously saved MBR has been corrupted, the following message is displayed:

1998—Master Boot Record has been lost.

1. Press any key to enter Setup to configure MBR Security.
2. Upon entering Computer Setup, you must disable the MBR Security feature.

You must know the Supervisor password, if one exists.

Before You Partition or Format the Current Bootable Disk

Ensure that MBR Security is disabled before you change partitioning or formatting of the current bootable disk. Some disk utilities, such as FDISK and FORMAT, attempt to update the MBR. If MBR Security is enabled when you change partitioning or formatting of the disk, you may receive error messages from the disk utility or a warning from MBR Security the next time the computer is turned on or restarted.

To disable MBR Security, complete the following steps:

1. Turn on or restart the computer. If you are in Windows, click **Start > Shut Down > Restart.**
2. As soon as the computer is turned on, press and hold the **F10** key until you enter Computer Setup. Press **Enter** to bypass the title screen, if necessary.

✎ If you do not press the **F10** key at the appropriate time, you must restart the computer and press and hold the **F10** key again to access the utility.

If you are using a PS/2 keyboard, you may see a Keyboard Error message—disregard it.

3. Select **Advanced BIOS Features > MBR Security** and press **Enter.**
4. In the MBR Security Pop-up box, use the down arrow key to select **Disabled.**
5. Press **Enter.**
6. Before exiting, click **Save & Exit Setup.**

Cable Lock Provision

The rear panel of the computer accommodates a cable lock so that the computer can be physically secured to a work area.

For illustrated instructions, please see the *Hardware Reference Guide* on the *Documentation CD*.

Fault Notification and Recovery

Fault Notification and Recovery features combine innovative hardware and software technology to prevent the loss of critical data and minimize unplanned downtime.

If the computer is connected to a network managed by HP Client Manager Software, the computer sends a fault notice to the network management application. With HP Client Manager Software, you can also remotely schedule diagnostics to automatically run on all managed PCs and create a summary report of failed tests.

Surge-Tolerant Power Supply

An integrated surge-tolerant power supply provides greater reliability when the computer is hit with an unpredictable power surge. This power supply is rated to withstand a power surge of up to 2000 volts without incurring any system downtime or data loss.

Thermal Sensor

The thermal sensor is a hardware and software feature that tracks the internal temperature of the computer. This feature displays a warning message when the normal range is exceeded, which gives you time to take action before internal components are damaged or data is lost.

Index